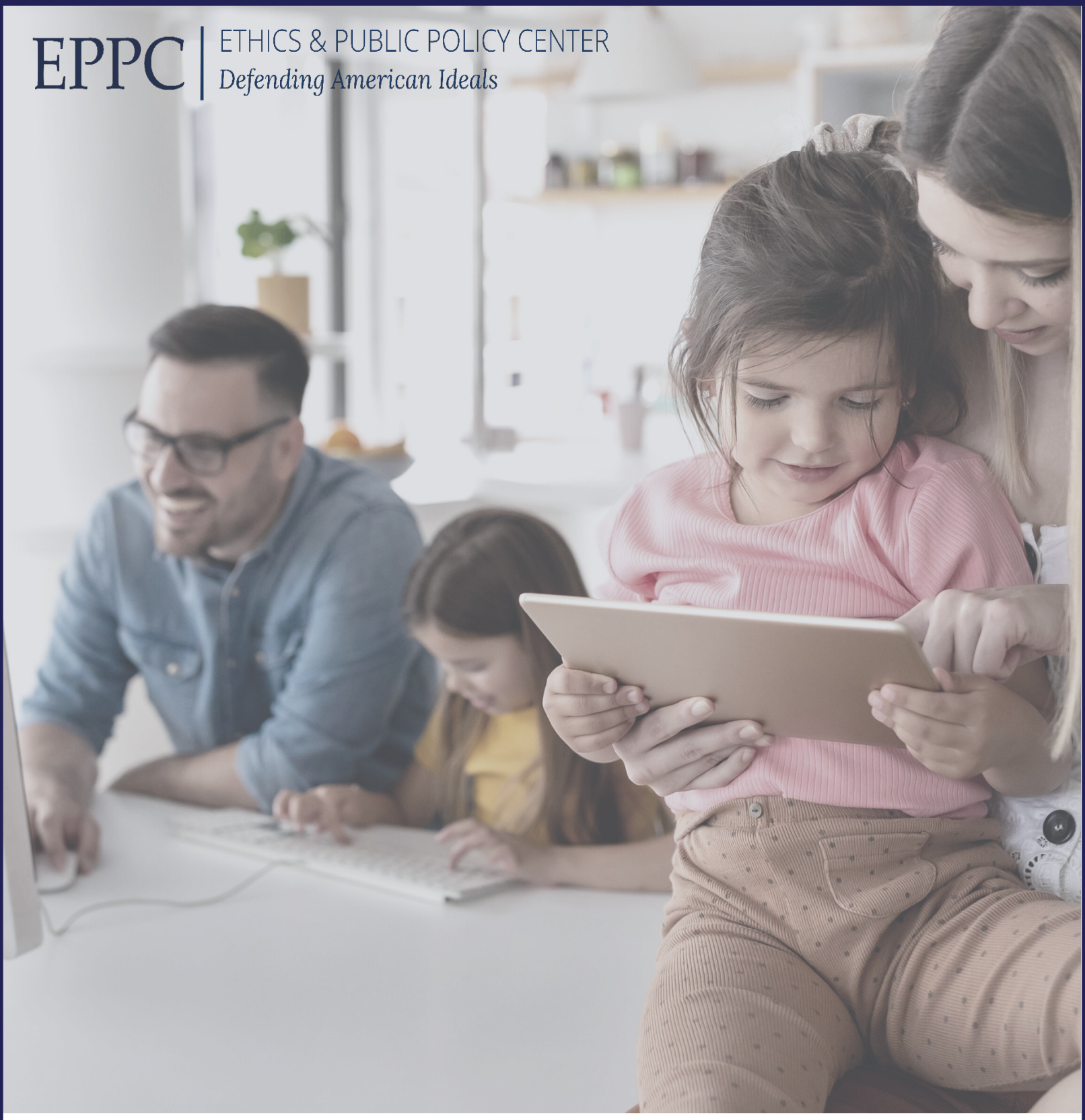
EPPC | ETHICS & PUBLIC POLICY CENTER
Defending American Ideals



RAISING A FAMILY IN THE DIGITAL AGE

A TECHNOLOGY GUIDE FOR PARENTS

The purpose of this guide is to educate parents and other adults working with and mentoring children (such as pastors, teachers, coaches, etc.) on the real threats and harms that today's social media platforms and digital technologies pose to our children and to equip parents with practical tools and resources to help them best protect their children. This guide offers both suggestions on boundaries to put in place around technology and how to have conversations with children about developing healthy habits with technology. This guide also explains practical tools and resources that are available to parents to protect their children, like parental controls and other protective software or apps, as well as alternative technology options that are safer than others for children to use. We hope this guide will help in navigating the challenges of parenting in today's digital age and empower parents with the knowledge and tools they need to best protect their children.

This guide was written by Clare Morell, Patrick Brown, Noelle Mering, and Mary Hasson.
Layout and design by Ella Sullivan Ramsay.
Editing by Josh Britton.

Step One:
Be Fully Aware of the Dangers

The rise of the smartphone and its accompanying apps, in particular social media platforms, are a primary source of many dangers to children today. The issues are two-fold. First, these apps and platforms often allow content that is harmful to minors to proliferate and then do little to nothing to remove it. Secondly, the nature of these platforms themselves are designed to be extremely addictive, causing negative effects on children's and teens' mental health and development, particularly teenage girls.

The *Wall Street Journal's* Facebook Files series has demonstrated the harms of Facebook and Instagram on teens' mental health, especially teen girls. Reports have also shown how TikTok and its algorithms serve up dangerous content to minors, sending them down rabbit holes of sexual and drug-related content. For example, a minor's "account was bombarded with marketing for strip clubs, promoted paid pornography and videos pushing the user toward OnlyFans.com, a platform favored by sex traffickers, with explicit sex and prostitution come-ons. Yet another account was lured into a TikTok space called 'KinkTok,' featuring torture devices, chains, whips and such. That these videos were labeled 'Adults Only' did not keep them out of minors' accounts." As Grazie Christie writes in the New York Post, "When a child starts watching TikTok footage of frolicking puppies or innocently dancing 12-year-olds, the site's algorithms go to work, continuously filling the feed. If she lingers for a few seconds on a video with even a subtle sexual or drug-related text or image, TikTok barrages her feed with ever-stronger content. From adorable animals to kinky sex, from droll dances to drug dealers, TikTok rapidly takes children down dark rabbit holes that would shock the most jaded adults."

And a *Forbes* review of hundreds of recent TikTok livestreams reveals "how viewers regularly use the comments to urge young girls to perform acts that appear to toe the line of child pornography — rewarding those who oblige with TikTok gifts, which can be redeemed for money, or off-platform payments to Venmo, PayPal or Cash App accounts that users list in their TikTok profiles. It's 'the digital equivalent of going down the street to a strip club filled with 15-year-olds,' says Leah Plunkett, an assistant dean at Harvard Law School and faculty associate at Harvard's Berkman Klein Center for Internet & Society, focused on youth and media. Imagine a local joint putting a bunch of minors on a stage before a live adult audience that is actively giving them money to perform whatever G, PG or PG-13 activities they request, she said. 'That is sexual exploitation. But that's exactly what TikTok is doing here.' The transactions are happening in a public online forum open to viewers almost anywhere on the planet." TikTok and Instagram also have both been shown to promote dangerous eating disorder content for girls, contributing to a wave of eating-disorder cases spreading across the country.

Let us be clear: today's teens don't need to go looking for it, dangerous, inappropriate content finds them on social media. Parents should be aware that simply by virtue of setting up an account on particular apps, harmful content (and contacts from bad actors) will automatically be pouring into kids' phones.

It is important to note that TikTok is also owned by the Chinese Communist Party-affiliated company ByteDance. There have been reports of TikTok sharing user data with the CCP through TikTok. Thus, TikTok is not only explicit (it is the worst app for serving up explicit content unbidden to children) but it is also very 'leaky' with user data.

The latest emerging threat is the virtual world, with virtual chat apps and gaming platforms. The gaming platform Roblox, rated as suitable for children as young as seven, made headlines for allowing virtual sex parties with bondage acts and strippers. Another virtual chat app, VRChat, has allowed minors to go into virtual strip clubs and see simulated sex. Youngsters can 'get naked and do unspeakable things' or take part in 'erotic role-play' in the apps. They are able to watch pole-dancing and mix freely with adults, which has led to grooming, racism and rape threats.

Let us be clear: today's teens don't need to go looking for it, dangerous, inappropriate content finds them on social media. Parents should be aware that simply by virtue of setting up an account on particular apps, harmful content (and contacts from bad actors) will automatically be pouring into kids' phones.

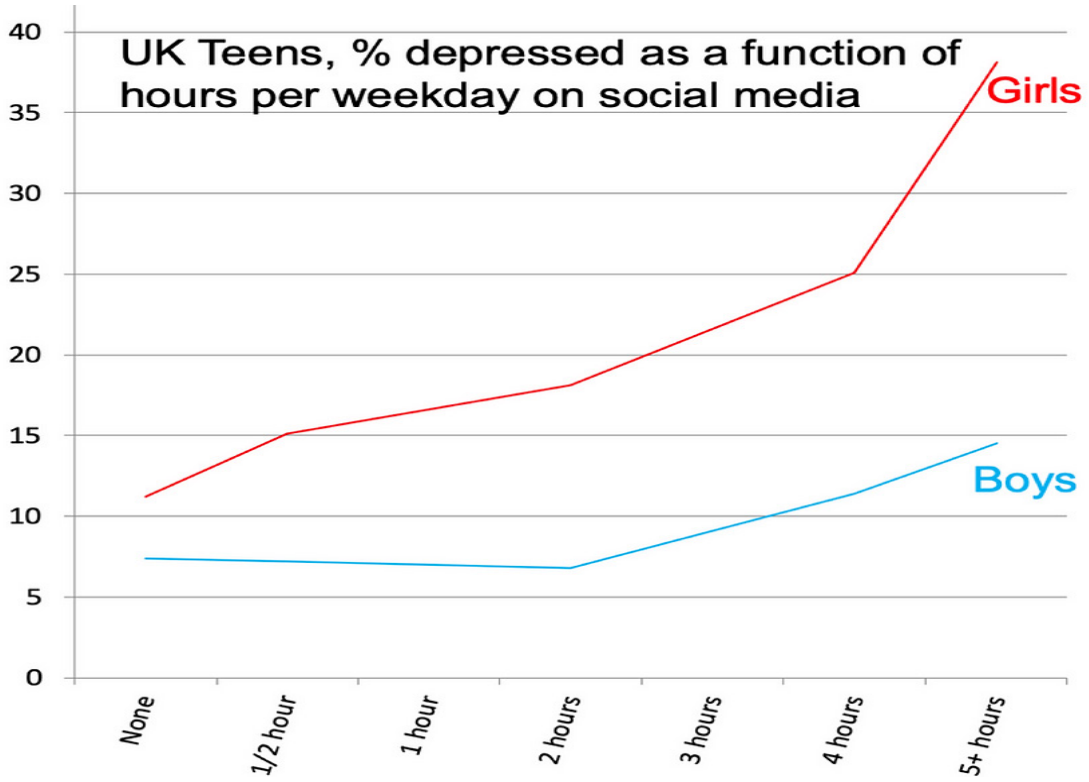
Social media platforms are often exploited by bad actors to harm children. Peers and classmates use them to engage in cyberbullying. For example, middle-school students are creating anonymous Instagram accounts called "spilling the tea" accounts that are used for gossip and cyberbullying. Even after kids leave school for the day, bullies follow them home through these online platforms. Even more nefarious, criminals like human traffickers use social media platforms to find and lure victims. Traffickers can now reach out to children on any application that allows for direct messaging. This includes apps like TikTok, Instagram, Facebook, Pinterest, SnapChat, Twitter, Roblox, and Fortnite. Any online platform where your children are interacting with their peers, even gaming communities, you should assume traffickers are on it too.

Furthermore, the rise of the internet, smart phones, and social media, have brought about a dangerous epidemic of online pornography, affecting in particular young adults but also minors. They now have 24/7 access to infinite content at their fingertips. And today's kids are routinely consuming violent, perverse, "kinky," demonic porn, some of it with interactive features so that they actually participate virtually in it. Much internet-based porngrapahy has grown more extreme, more violent, and more misogynistic and degrading towards women, and includes homoerotic and

now "sissy" porn (transgender porn). The danger of online pornography today is not just more pervasive, it's more extreme and different in kind from what was out there even five years ago. Social media apps are often the entry point to pornographic sites and they themselves distribute pornographic content on their platforms. Teens don't need to go looking for it, it finds them on social media.

Despite much silence on the topic from the mainstream media, trans influencers on social media are driving the disturbing transgender movement in teens. Social media sites peddle misinformation on the drugs and surgeries of the trans world and coach teens on how to lie to doctors and their parents in order to get them. These platforms are filled with confessional videos from influencers about how great they feel now that they have "transitioned."

Finally, beyond the harmful and disturbing types of content they distribute, the nature of the platforms themselves, designed to be highly addictive, is causing negative health consequences in children and teens. There was a significant increase in the rates of depression and anxiety among teens and it hit girls particularly hard, right around 2013 when Facebook bought Instagram and made it much more addictive. Between 2011 and 2018, the rates of depression, self-harm, suicides, and suicide attempts exploded among American teens. The rates of teen depression increased by more than 60 percent, with the larger increase among young girls. Between 2009 and 2015, emergency room admissions for self-harm among 10- to 14-year-old girls tripled, and suicides substantially increased. Correlation does not prove causation, but there are few plausible alternative explanations for the massive, sudden, multinational deterioration of teen mental health during the period right after the advent of social media.



"Greater social media use related to online harassment, poor sleep, low self-esteem and poor body image; in turn these related to higher depressive symptom scores." The correlation is greater for girls than for boys.

Numerous studies have linked time spent on social media with depressive symptoms.
This graph is from a 2019 study: Kelly, Zilanawala et al. (2019)

Step Two:
Set Appropriate Boundaries and Guidelines

How to Have Conversations with your Children about Technology:

It is easy to slip into a mindset that the safety of home is merely about what to keep out. Equally important, is a focus on what it is we are building within. Our children will be more motivated and inspired by a positive vision than a negative one. One way to do this is to encourage the development of interests that are natural to the child's personality and temperament. A child who loves video games might also love competitive sports or strategic board games. Similarly, love of stories can be fostered more through reading good books than the many vacuous shows on YouTube. Losing oneself in a story, musical instrument, or a nature walk is far more pleasant and rewarding than the constant self-awareness fostered by social media. Once kids discover that, then conversations can be more readily understood about spending time in ways that develop our virtues and skills and feel more fulfilling than whiling away hours on a screen. Fostering an environment of fun and cheerfulness in the home will go a long way to communicate to kids that it is truly for their good and happiness that such rules are in place.

The influence of friendships gains as children grow. It is helpful if possible to seek out communities in which adolescents will not feel odd or isolated if they do not have social media and smartphones. Such communities not only prevent the feeling of isolation, but they can also fill the formative role of positive peer influence reinforcing habits of life that lead to happiness.

Parents should strive to create an open door with their kids about technology. Conversations are crucial surrounding not only how children are utilizing technology, but also about the type of content that they can access. This often will mean speaking to them earlier than we might like (sadly the average age of first exposure to pornography is 9 to 11 years old and it is often accidental exposure),

but it's so important to do because if they're not learning something from you, then they'll go to their peers or search it on Google. Urge them to talk to you (even if they feel embarrassed) if they ever view something confusing or that just doesn't seem right. The organization, Protect Young Eyes, recommends "10 Before 10" - having ten talks about pornography with your child before the age of 10. Each conversation is just the repetition of letting them know if they come across naked people or anything that makes them uncomfortable on the internet that you are a safe space, you won't freak out, they can talk to you about what they saw.

If you decide to use parental controls, talk to your kids about why you're using them (to foster their long-term happiness) and how your ultimate goal is for them to learn how to communicate and interact with other people in a productive way and to regulate their online usage responsibly and independently.

And lastly, the most important thing you can do as a parent is model good use of technology for your children. Recent studies have shown that rates of depression were higher among teens whose parents reported high levels of social media use. A Washington Examiner article pointed to a study from the Wheatley Institute that found, "Adolescents are nearly four times as likely to be depressed if their parents are high level social media users".

Additionally, minimizing time on phones or screens as adults sets a good example for children. Being present with them when they wake and after school provides the space for meaningful conversation as well as the various small conversations that establish and reinforce parent/child connections. Also important is the modeling of positive uses of technology as a family for shared experiences, like watching a movie together on the television or playing a trivia game online together, etc. Model how you can use technology to bring the family together, rather than allowing it to divide you by everyone being on their own screens.

Sample Boundaries:

Parents need to figure out how to adopt healthy boundaries on technology for their family. As Canopy CEO Sean Clifford has said, "that really begins by thinking of a device, whether it's a smartphone or a tablet or a computer, as akin to a car. You don't just hand over the keys to a 7-year-old and hope for the best. You gradually teach them how to use it responsibly, make them aware of some of the dangers they might encounter out there, with the goal that ultimately they have the independence and the excitement that comes from having the run of the road."

Here are just a few ideas of possible boundaries to consider:

- Children and teens can only access the internet from a family computer or tablet used in a common space where they can be seen. If they have a school-given laptop or tablet, do not trust the filters on a school device and have them use that device only in common areas where you can see what they are looking at.
- No devices or screens - computers, tablets, or phones - in children's bedrooms. Especially not at night.
- No devices at the table. Share meals together around the table without phones present.
- Have a phone basket where everyone, including parents, put their phones once they come home from work and school to create time for in-person interactions as a family in the evening.
- Parents should make sure to have passwords set up on all their devices that the children do not know. Including putting password protection on the family computer, so that parents have to log kids on when they want to use the internet.
- Use parental controls to restrict access to the computer and the internet to times when a parent is home and around to supervise what kids are doing.
- Ask your internet service provider (ISP) about filtering software that may be available to you (see options below).
- Set daily time limits for each child and each device for screen time.
- Train your children for how to handle technology when they are outside the home, at a friend's house or school. For example, if you don't allow your child to have a smartphone you can create a family rule to not look at smartphones. So if a friend is offering to show your child something on a screen they can simply say "No thank you, in our family we don't look at phones."
- Consider the idea of a tech-free Saturday or Sunday where everyone turns off their devices for the entire day to create time and space to be together and spend time doing shared activities together as a family. This can help everyone relax and disconnect from the constant stimulation of devices and be a mental reset. It also helps teach your children that there is a time and place for technology and it does not need to be used constantly or always on.

Social Media Safety Guidelines:

Despite varying degrees of pressure, there is no real need for parents to allow their kids to have social media accounts. Beyond the more sinister dangers highlighted earlier, there is the exacerbation of normal insecurities of youth brought on by measuring the ways in which they and their peers are "liked" or not "liked" on each and every post. Additionally, the tendency to publicize every social occasion brings a layer of performativity to the soul which can hinder the true development of virtue and cement in a teen a fragile sense of self.

There certainly may be practical challenges to not allowing your children to have such accounts, but they should be balanced by a recognition of the enormous dangers, harms, and social pressures that are introduced by having them. At best, it is far easier to delay their introduction than it is to cancel them once introduced.

Minimizing the amount of technology, particularly social media, until children reach or are closer to adulthood is ideal. Even the most tech-aware and vigilant parents can't always keep tabs on everything their child is doing online. Some families may benefit most from deciding their teen doesn't need access to social media at all, and restricting their access until they turn 18 *(** in particular, TikTok is the worst app for serving up explicit content to children unbidden, so we would strongly recommend that parents not permit any child or teen under 18 to have a TikTok account **)*. Others might work out an arrangement in which their child can sign up for an account at 16, but is required to share all their password and log-in information with their parent, who can then see what their child is seeing and who they are interacting with. If and when you do choose to allow your teen to have social media:

- Set any privacy settings to the strongest possible if you allow your child to use a social networking site and limit their friends list to people they know. Accounts for children should always be set to private.
- It could also be wise to have your child not use his or her real name and to talk to them about being careful with any photos they post, messages they send, etc.

It is also worth noting that many schools are now requiring students to use certain technologies in the course of their schoolwork. While the exact technology might vary from school to school and district to district, parents should not assume that schools are enacting appropriate filtering devices. Many of the practices in this guide mentioned above, such as collecting devices at the end of the day and not using them in private spaces, can help buttress any policies, procedures, or filters the school offers.

Minimizing the amount of technology, particularly social media, until children reach or are closer to adulthood is ideal.

Step Three:
Utilize Helpful Tools and Alternatives

The below are examples of tools parents could utilize for their families. We are not recommending or endorsing any one tool over another. Tools also are not a silver bullet. Protecting children will take a combination of setting good boundaries, as mentioned above, utilizing tools where needed, and monitoring our children and any online behavior they are allowed to have.

Parental Control Software, Hardware, and Apps:

Click on the logo to learn more

CANOPY

Highlights

- ✓ Blocks all explicit images and videos on web browsers
- ✓ Allows Parents to block apps
- ✓ Scans and analyzes photos taken on a child's device

- Canopy's SafeSmart Internet Filter uses artificial intelligence to scan, detect, and eliminate explicit content on web browsers in milliseconds, before it reaches your child's screen. It blocks inappropriate images and videos in web browsers, replacing them with harmless white rectangles. It makes real-time decisions about content, and doesn't rely on an incomplete or outdated list of inappropriate sites. Canopy filters all websites but does not filter inside apps (like Snapchat and Instagram). No other parental control app can filter in apps either.
- Canopy does give parents the power to block any app they think isn't right for their family. Canopy allows parents to decide which apps are right for each child and device. With its App Management tool, you can easily cut off internet access for specific apps or games while still letting your child access their device's productive features.
- Canopy also automatically scans and analyzes photos that are taken on your child's device, as well as photos that are downloaded to your child's device. If it detects a potentially problematic photo, Canopy immediately prevents your child from accessing or sharing it until it is reviewed by you, the parent. Canopy gives your child the option to keep or delete the photo. If they choose to keep it, the photo will be sent to you for review. They cannot access the photo while waiting for parental approval. You review the photo from your personal device and decide whether to allow it or delete it. If you delete it, Canopy will force the photo to be deleted from the child's device.

Highlights

- ✓ Full device screen monitoring for Android
- ✓ Online activity is reported with explicit content flagged
- ✓ Blocks millions of explicit websites

- Covenant Eye's philosophy is based on accountability. They believe that more than technical solutions are needed because access is not the only problem to address in fighting pornography. Their solution is to provide tools to bring honesty and transparency to accountability relationships. With Covenant Eyes, you invite someone you know and trust to hold you accountable. For families then, parents serve as children's best ally on their journey to quit porn or never start. Screen Accountability helps parents have honest conversations that heal shame and strengthen their relationship with their kids, while the Safe Search and filtering tools keep porn at bay. The three main tools Covenant Eyes provides are:
- Monitoring - Monitoring brings objectivity to accountability conversations.Full device screen monitoring on Android tracks activity in all apps. In-browser screen monitoring on iOS tracks activity in the Covenant Eyes app. Full device screen monitoring on desktop computers
- Reporting - Online activity is packaged in an easy-to-read report and sent to the accountability ally. Patented AI flags explicit content for review. Easy-to-read summary of cross-device activity. Reports use blurred screenshots sent with 256-bit AEP encryption to protect your privacy
- Blocking - Preventing triggers is an important part of porn recovery. Clean Browsing-powered domain blocking eliminates millions of explicit websites. Custom block and allow lists give administrators control of what is filtered. Safe Search protects all major search engines and YouTube from explicit content

**Note: Due to Apple restrictions, Screen Accountability is only available on the Covenant Eyes app. Screen Accountability is currently unavailable for Chromebooks, Kindle Fires, and Smart TVs.

Highlights

- ✓ Screentime management & website monitoring
- ✓ Ability to restrict or block apps and webpages
- ✓ Can be activated on individual devices or wifi network

Circle offers parental controls to manage screen time and monitor all websites and apps for your family. By setting up the Circle content Internet Filter feature, parents can easily select the apps, devices, games, streaming services, and websites that need limitations or restrictions. Then, add filters to each family member's profile accordingly. Each profile is easy to manage, no matter where you are. Just open up the app, and you can change Internet filters with a few taps on your phone. Circle's Internet filtering software works anywhere. You can use the parental control app as an Internet filter for iPhones and Android devices, and with the Circle Home Plus device, you get a

whole house Internet filter on your Wi-Fi network.Circle uses a database loaded with millions of websites, and bundles them into a few easy-to-understand categories, like Social Media or Education or Online Games. You can filter Internet content and apps by category or by individual websites and apps/platforms. Within the default settings for each age, platforms and categories can be toggled to allowed, not-allowed, or "unmanaged." Content that is "allowed" is available for their use, and you can customize Time Limits as well. On the flipside, content that is "not allowed" will not be available online, no matter what. So, if you want to make sure your tween cannot access YouTube at all, you can toggle to "Not Allowed" for that app. When you choose the "unmanaged" option that means the selected content is always 100 percent available and not tracked in Usage/History. If you want to get more specific with what your kids can access on their devices, you can make a Custom Filter and add individual websites to either allow, filter out, or unmanage entirely. Circle also offers Safe Search and YouTube Restricted Mode, which automatically eliminate sexually explicit content from search results.

bark

Highlights

- Monitor texts, youtube, email, and more...
- Alerts parents of suspicious/dangerous device use
- Manage screentime and set restrictions

Bark allows parents to monitor text messages, YouTube, email, and over 30 different social media networks for potential safety concerns based on the child's usage and interactions. Bark's monitoring program also looks for any language or image sharing that may indicate communication with an online predator and alerts the parents. Bark also offers screen time and web filtering. Families can manage when their kids can access the internet on their devices, as well as which sites they're able to visit. They can set bedtimes and block access to a wide variety of websites — including streaming, gaming, and adult content, and more. Bark allows parents to: manage screen time, filter which websites kids can visit, keep up with kids with location check-ins, monitor texts, email, YouTube, and 30+ apps and platforms, and get alerts for issues like cyberbullying, online predators, suicidal ideation, and more.

Qustodio

Highlights

- Monitor child's apps, social media, and internet
- Block or set alerts for certain words, websites, and apps
- Set time limits and track devices via GPS

Qustodio's app is an all-in-one parental control system that allows you to monitor your child's device use and manage their web access. You can track the websites visited, apps used and even the social media activity of your child. The social media feature only works fully for Facebook and YouTube, but you are able to track the time spent on other platforms such as Twitter, Instagram, and WhatsApp. For Android phones, the app gives you the power to track calls and SMS text messages. As for the restrictions you can set, you can block certain words, websites, apps and set-

time limits for each day. You can easily customize the app to set limits for your children or leave it to the automatically enabled, powerful filtering technology to take care of it for you. You can set the app to deal with the filtered words and URLs in three different ways: allow, block or alert. Alongside offering the complete package in supervising online activity, Qustodio also comes with other advanced features for your child's protection. They have a locator feature that finds iOS and Android devices on the map, this includes a geo-fencing feature and an SOS button for Android devices which sends the parents a location-based alert if there's trouble.

Net Nanny®

Highlights

- ✓ Blocks inappropriate or dangerous content
- ✓ Screen time management and parental controls
- ✓ Location tracking

Net Nanny's content filtering technology offers a solution for browsing the Internet and blocking inappropriate or dangerous content, while still allowing your family access to appropriate websites. Net Nanny's parental control software offers a variety of functions, across multiple devices, all created to enrich and safeguard your family's online experience. Net Nanny has many features including parental controls, location tracking, app blocking, website blocking, Internet filtering, porn blocking, alerts and reporting, and screen time management.

CleanBrowsing

Highlights

- ✓ Content filtering that blocks porn and obscene content
- ✓ Block content based on category
- ✓ Customizable to your specific needs

CleanBrowsing is a content filtering service that blocks access to porn and obscene content on networks. It is a DNS-based filtering service, which is a cloud-based solution that is platform agnostic (i.e., Apple, ChromeBook, Windows, etc.). DNS resolvers are a core piece of how the internet works. Every device connecting to the internet makes use of DNS. Leveraging this technology allows them to provide a installation free cloud service that can filter requests made to the internet from your device or network. It uses both DNS and content filtering. DNS Filtering is a content filtering service that relies on the Domain Name System (DNS) to block, or allow, content on a specific network. DNS offers users, and organizations, the ability to apply access rules across all devices independent of the OS or browser type. It is not tied to a specific technology, and it's at the core of how the web works. Content Filtering is a mechanism that allows you to proactively decide what should, and should not be allowed on your internet. Organizations can build acceptable use policies with this technology, parents can control what their kids access, and municipalities can create family friendly hotspots. They have over 19 predefined filters so you can quickly filter entire categories (e.g., Pornography, Partial-Nudity, Malicious, Mixed Content, etc.). And you can also easily add custom domains to the custom "allow" or "block" lists to create custom rules on your network.

GRYPHON®

Highlights

- ✓ A parental control Wi-Fi router
- ✓ Content filtering based on user's age
- ✓ Screen time monitoring and ability to disable internet

Your router is the most important digital device in your home. Many parents today are frustrated with the battle to protect their children from the dangers of being exposed to inappropriate online content, excessive screen time, and social media addiction. The Gryphon Parental Control Router puts the control back in parents' hands. Using the Gryphon Connect App, parents can manage their childrens' online activities and ensure healthy amounts of screen time from anywhere you go. It allows parents to set content filtering based on a user's age, with 1.2 million blocked sites stored locally on Gryphon, and aggregated website reputation ratings from multiple sources including other parents. It also allows parents to monitor their child's browsing history even if they delete it. As well as schedule screen time for your children in the run up to automatically shutting off their internet for bedtime. And with the touch of a button, parents can shut off the internet, giving you instant and non-negotiable family time.

Built-In Parental Controls

Major Internet Service Providers

Many internet service providers, device manufacturers, and content providers include parental controls, some of which are easy to use, and some are not. In general, the best way to discover the different capabilities of devices or platforms to enact parental controls is to search for the device's user manual.

The capabilities of each approach to parental controls can range in comprehensiveness, from turning off wi-fi access to certain hours, to relying on the manufacturer/platform's ratings for age-appropriateness. It goes without saying that certain messages and contents may be deemed appropriate for a certain age level, but be inappropriate for individual kids.

Most parental controls rely on a PIN or password to access. If children gain access to these log-ins, they can easily override parental controls (in fact, some websites offer technical hacks for children to attempt to get around them). Not every device or software will notify users that settings have been changed, so parents shouldn't rely solely on the device or manufacturer's controls. Parents should know how to regularly review their children's activity and check their network's security settings.

Internet Service Providers
Parental Controls Comparison Chart

Click on the title of the company to learn more

AVAILABLE CONTROLS	AT&T	COMCAST	VERIZON (SMART FAMILY)*	CHARTER/ SPECTRUM
Block websites	✓	✓	✓	✓
Monitor web use	✓	✗	✓	✓
TV content locks	✗	✓	✗	✗
Set time limits	✓	✗	✓	✓
Can be used remotely	✓	✓	✓	✗
Restrict certain times	✓	✗	✓	✓
Block based on category	✓	✓	✓	✓

*costs $5-10/month

Video & Streaming Content

When it comes to movies, the Motion Picture Association ratings (G, PG, PG-13, and R) have long been known to be insufficient when it comes to fully informing parents' choices. Certain parents may have a different level of perceived appropriateness when it comes to depictions of violence, drug use, sex and/or nudity, or other material than the official rating suggests. Two websites that offer a more detailed look at what types of objectionable content are in a movie or TV show are Plugged In and Kids in Mind. Each of the major streaming services offer content filters as well, though of course they do not give parents the ability to know what sort of messages are being pushed in each movie or TV show, which parents may be concerned about.

Video & Streaming Services Parental Controls Comparison Chart

Click on the title of the company to learn more

AVAILABLE CONTROLS	AMAZON PRIME	NETFLIX	HULU	GOOGLE PLAY	DISNEY+
Kids Profile	✓	✓	✓	✗	✓
Content restriction	✓	✓	✓	✓	✓
PIN required to access restricted content	✓	✗	✓	✗	✓

Smart Devices

Apple devices:
With Content & Privacy Restrictions in Screen Time, you can block or limit specific apps and features on your child's device. You can also restrict the settings on your iPhone, iPad, or iPod touch for explicit content, purchases and downloads, and privacy. More information about parental controls on Apple is available here.

Android devices:
Because there are a wide variety of manufacturers that make Android devices, the easiest way to ascertain what parental controls are available is to search for the user's manual for a given device. Google offers some general guidelines on parental supervision for its products.

Search Engines

Bing:
To filter out adult text and images from Bing search results, select the settings icon in the upper right of the Bing.com window, then select "More." Choosing "strict" will filter out adult content from search results, but will not filter out other websites. Select Save at the bottom of the menu. (Be aware that even when using Bing's filter there can still be problematic search results with thumbnail images. Even if a child can't click through to the explicit site, thumbnails can sometimes be explicit.)

Google:
Google's SafeSearch setting can help you filter explicit content from your results. Explicit results include sexually explicit content like pornography, violence, and gore. SafeSearch only works on Google search results. It won't block explicit content you find on other search engines or websites that you go to directly.

DuckDuckGo:
DuckDuckGo's safe search setting lets you to remove adult content from results on DuckDuckGo. You can activate it in the following ways:

- With the dropdown box under the search box in their results pages.
- With the "Safe Search" option in the DuckDuckGo settings page.
- By appending !safeoff to your search (this uses their bang syntax).
- By using safe.duckduckgo.com instead. Searches from safe.duckduckgo.com always have safe search set to "strict".

App Stores

The Apple App Store and Google Play both require apps to be rated according to certain categories, and parents are able to determine which age category their child is allowed to download. As with video game and movie ratings, each parent's comfort level with violent or suggestive content may vary from the certification given to it by developers, so parents should not necessarily trust that an app okayed for teens will be free of content they would find objectionable.

Popular Apps

Instagram:
Meta has recently begun to offer parental controls. They now offer a Family Center for Instagram where parents can send invitations to supervise their teen's Instagram account and stay up to date on who they follow and who follows them, as well as see their teens' daily average time spent on Instagram and help manage their time by setting time limits together. Parents can designate quiet hours for each day or week and if their teen reports an account or post for inappropriate behavior, the parents will be able to see more information, such as the type of report and the account that was reported. While less than desirable that teens have to approve their parents' request for these parental controls, it is a start. Be aware that teens can also revoke parental-control permissions at any time, but doing so triggers a notification to the parents.

TikTok:

Family Pairing is a parental control feature on TikTok that allows a parent to link their TikTok account to their teen's account and set controls for the following: **(the down side is this requires the parent to make or have a TikTok account; also TikTok is the worst app for serving up explicit content to children unbidden, so we would strongly recommend that parents not permit any child or teen under 18 to have a TikTok account **).

- Screen Time Management: Choose how much time your child can spend on TikTok each day.
- Restricted Mode: Make certain content subject matter off-limits.Search: Decide what types of content, users, hashtags, or sounds your kid can search for
- Discoverability: Set your child's account to private or public.
- Suggest account to others: Choose whether your kid's account can be recommended to others.
- Direct Messages: Kids aren't allowed to direct message (DM) until they turn 16. DMing is automatically turned off for users between the ages of 13 and 15.
- Liked videos: Decide who can view the videos your teen liked.
- Comments: Choose who can comment on your teen's videos.

To turn on Family Pairing:

- Go to your profile page or your child's profile page; click on the three dots that are located in the top right-hand corner, select Family Pairing, and follow the steps in the app.

You can also set up Screen Time Management for your child:

- Go to your child's profile page.
- Click on the three dots that are located in the top right-hand corner and select Digital Wellbeing.
- Tap Screen Time Management and follow the steps in the app.

How to turn on Restricted Mode:

- Go to your child's profile page
- Click on the three dots that are located in the top right-hand corner and select Digital Wellbeing.
- Tap Restricted Mode and follow the steps in the app

Facebook:

There are no built-in parental controls available through Facebook. Instead, you'll need to adjust your child's General Account Settings to make sure their profile is as protected as possible. Walk your child through the General Account Settings to help protect them from the worst of what can happen on Facebook.

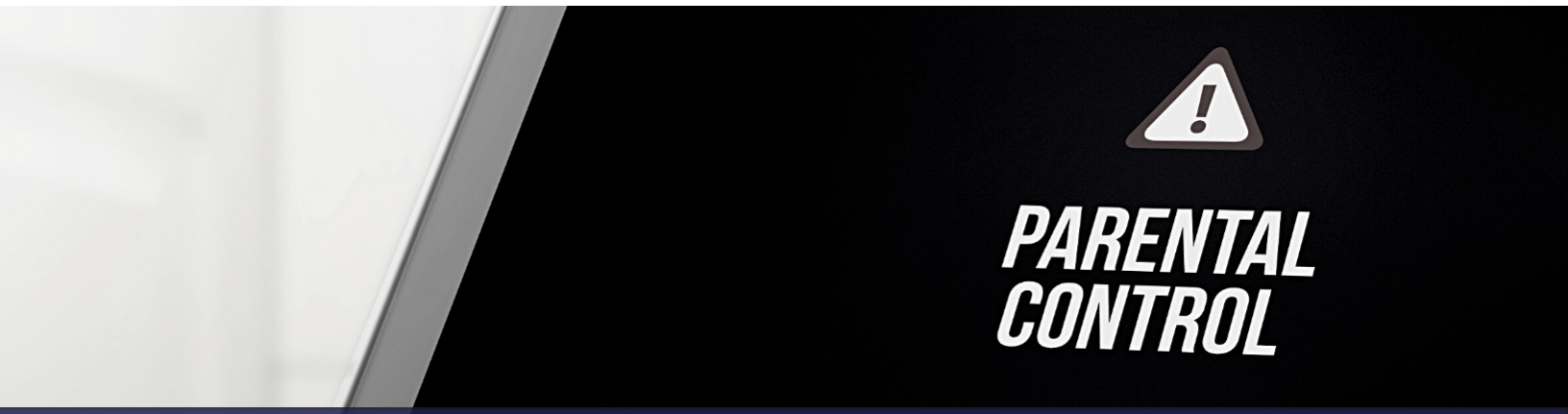
- Log in to your child's Facebook account. Select Settings. A column of Privacy and Security options will appear.
- General: Allows you to change your child's contact information, direct notifications to your own inbox, and deactivate the account if necessary.

- Security and Login: Allows you to change your child's password, set up two-factor authentication, and authorize devices that don't require passwords to log in to the account.
- Your Facebook Information: Allows you to view, download, and delete your child's personal information from Facebook.
- Privacy: Allows you to determine whether your child's profile is "Public," available only to Friends, or even a customized selection. You can manage who can see their account activity, can send them friend requests, and use their personal information to find and contact them. You can also prevent your child's profile from appearing in search engine results.
- Timeline and Tagging: Allows you to adjust whether other people can tag your child in photos or posts of their own, as well as reviewing posts they're tagged before it appears on their timeline.
- Blocking: Allows you to block someone from viewing your child's posts or send messages or event invites. You can also block entire pages.
- Face Recognition: Allows you to set whether or not you want Facebook to be able to recognize you in photos and videos.
- Public Posts: Allows you to regulate access to your child's public posts, including who can follow them and who can like or comment.

YouTube:

Parents on either iOS or Android can give their kid a supervised account for YouTube viewing. This YouTube video and help page explains how. You can also download Google's Family Link app, which lets you set screen-time limits on YouTube and other apps on your child's Android and Chrome devices, and to manage other online activities. (For YouTube alone, Family Link isn't required.) Supervised YouTube accounts offer three different content settings: One allows kids to watch channels approved for viewers 9 and older, with no live streams. The second grants access to channels deemed appropriate for kids 13 and up, including live streams. And the third option lets them watch anything that isn't labeled 18+. Parents can also block specific channels on supervised accounts.

For those 13 or older, parents can use restricted mode, which helps filter undesirable content, directly in the YouTube app or browser. You will have to do it wherever the kid is logged in—and note that your kids can undo it.



**For a comprehensive list of parental control options see Internet Safety 101's page here. Protect Young Eyes also has parent guides for how to set up parental controls on most digital devices, as well as reviews of all the most popular apps being used by kids today so parents can better understand how each app works and its potential dangers to kids. **

Phone Alternatives

The Light phone:

The Light Phone II won't allow your child to get on the Internet or social media, but it will allow him to call and text (including group chats) on the AT&T network, as well as access simple tools like an alarm, calculator and music/podcast player. The device currently doesn't offer GPS tracking.

Sunbeam Wireless F1 Phone:

The F1 cellular phone from Sunbeam Wireless is a flip phone that gives the tools you need, but without the distractions and potential dangers of most modern devices. There are three models available, none of which have email, a web browser, or an app store/apps/social media:

Dandelion Model: The Dandelion is a phone that offers talk only. Free from text messaging and media player.

Daisy Model: The Daisy offers talk and text. It has SMS/MMS messaging capabilities, but no extras.

Orchid Model: The Orchid offers talk, text, as well as added features like weather and navigation. But still has no browser or social media.

Tick-Talk Phone Watch:

TickTalk 4G/LTE smartwatch phones are designed for kids ages 5-12. TickTalk smartwatch phones don't have internet, social media or games. The smartwatch phone allows parents to call their child, video chat, send photos, text messages and track their location. TickTalk's Secured/Encrypted end-to-end Individual & Group Chat messaging makes sure no one can read or edit the messages you send your child as they travel between your phone or device and your child's TickTalk smartwatch phone. TickTalk smartwatch phones for kids have 2-way voice calling, HD video calling, Talk-To-Text, unlimited preset /customizable quick text responses and voice messages. TickTalk gives you the ability to set Emergency SOS contacts, block unknown numbers, approve contacts, view call logs and SMS text requests and more. Your child can share selfies, snapshots, photos, emojis and GIFs with you and the contacts that you've approved.

GizmoWatch 2:

Exclusive to Verizon customers, the GizmoWatch 2 lets kids keep in touch with 10 approved contacts and comes with GPS tracking. Parents, you have to use the GizmoHub app to text the watch from your own phone, there is no group texting and your child can only text a pre-written phrase, emoji, or voice message.

The Gabb Phone:

Designed to mimic the appearance of an iPhone or Android (but without access to internet, games or social media) the Gabb is great for kids concerned with being the odd one out. It also has an accessible price and plethora of parental controls—from screen-time limits to GPS tracking. The phones run on Gabb's own 4G LTE network, no contract required. Gabb also offers a warch phone for kids.

The Pinwheel Phone:

Pinwheel phones access neither the internet nor social media, but offer their own age-appropriate, nonaddictive apps like a virtual journal, e-reader and Duolingo language app. Parents use a companion app on their own phones to choose different modes like "school mode" or "free play mode" that allow or block features. Only whitelisted contacts (approved by a parent) can interact with the child.

Smart Phone Alternatives Comparison Chart

Click on the phone name to learn more

FEATURES	THE LIGHT PHONE	SUNBEAM WIRELESS F1	TICK-TALK PHONE WATCH	GIZMOWATCH 2	THE GABB PHONE	THE PINWHEEL PHONE
Cost	$299 plus plans from $30/month	$195 plus service plan	$165-$190 plus $10/month	$100 plus $10/month	$100 plus plans from $20/month	$149+ plus plans from $15/month
Age Range	Any	Any	Designed for kids ages 5-12	Recommended for ages 6-12	Recommended for ages 6-12	Recommended for Ages 5-17
Service Provider	Works with most major carriers	Works with most major carriers	works with AT&T and T-Mobile	Exclusive to Verizon	Gabb's 4GE network	Works with most major carriers
Call and Text	✓	✓	✓	✓	✓	✓
Group texts	✓	✓	✓	✗	✓	✓
Video Calls	✗	✗	✓	✗	✓	✓
GPS Tracking	✗	✓	✓	✓	✓	✓
Photo and Video	✗	✓	✓	✗	✓	✓
Other Features	Alarm, hotspot, music, directions	3 models, each with different capabilities	GIFs & emojis, parental control of calls and texts	Step Tracker, limited to 10 contacts	MP3, radio, bluetooth, alarm, voice recorder, calculator	Music, banking apps, remote management, school mode

Other Resources

Books:

- The Tech-Wise Family by Andy Crouch (for parents)
- Parenting Generation Screen: Guiding Your Kids to Be Wise in a Digital World by Jonathan McKee (for parents)
- 12 Ways Your Phone is Changing You by Tony Reinke (for parents)
- The Coddling of the American Mind by Gregg Lukianoff and Jonathan Haidt (for parents)
- iGen by Jean Twenge (for parents)
- Good Pictures, Bad Pictures by Kristin Jenson and Debbie Fox (for kids, ages 6-11)
- Good Pictures, Bad Pictures Jr. by Kristin Jenson and Debbie Fox (for kids, ages 3-6)

Articles:

- Facebook's Dangerous Experiment on Teen Girls, Jonathan Haidt, The Atlantic, November 21, 2021
- Have Smartphones Destroyed a Generation?, Jean Twenge, The Atlantic, September 15, 2017
- How to Protect Your Kids From Internet Porn: There's an App for That, Rob Bluey, The Daily Signal, Jan 31, 2022
- Why Device-Free Dinners Are a Healthy Choice, Michael Robb, Common Sense Media, August 4, 2016
- Five Digital Trends that Threaten Children in 2022, Chris McKenna, Protect Young Eyes, Jan 1, 2022
- Haidt, J., & Twenge, J. (2021). Social media use and mental health: A review. Unpublished manuscript, New York University.
- Parental Controls for the Internet and Cell Phones, Vincent Ianelli, MD, Very Well Family, December 21, 2020
- TikTok Brain Explained, Julie Jargon, The Wall Street Journal, April 2, 2022
- How to Use Parental Controls on YouTube, TikTok, Instagram and Snapchat, Julie Jargon, The

Websites:

- Protect Young Eyes
- Healthy Screen Habits
- The Coddling: Better Social Media